INTERNAL AUDIT
CONTROLS EVALUATION
OPERATIONS CENTER

June 2, 2003

Roanoke City Council Audit Committee
Roanoke, Virginia

We have completed an audit of the operations center. We performed this audit in accordance with generally accepted government auditing standards.

BACKGROUND

The Department of Technology is responsible for the overall management of Information Technology, Telecommunications (Radio Shop), and the E-911 Center. It has a $4,354,502 adopted budget for 2002-2003, of which $2,140,309 is related to personnel expenditures and $1,206,675 is related to operating expenditures. The Operations area of the Department of Technology is responsible for providing information system services to all city departments for the efficient operation of city government through on-line and batch support.

The Department of Technology has recently restructured its organization in an effort to provide more redundancy and back up capability among its staff. This should result in more fully cross-trained staff and provide employees with more opportunities for professional development and job advancement. The restructure has required the Operations area to take on additional responsibilities such as receiving help desk calls. As a result of the reorganization, the Operations area now has a total of nine positions including the Enterprise Operations Administrator, AS400 Systems Programmer, Security Administrator, Information Technology Coordinator, four Operations Support Specialists, and the Trainer position.

The Operations area is responsible for the physical security of the computer room, tape vault, and for restricting access to the Department of Technology's entire suite of offices after normal business hours. The computer room houses the mainframe computer system and 32 servers. The Operations Support Specialist's day-to-day duties include job scheduling, tape management, releasing jobs into production, and output distribution. In addition, the Operations area is responsible for the media center and the Department of Technology's disaster recovery plan. The media center has laptops, projectors, and other media equipment that departments can reserve and use as needed.

PURPOSE:

The purpose of this audit was to evaluate the physical security over the Operations area and to evaluate the controls over tape management, job scheduling, output distribution, job releases, and the media center. We also wanted to specifically evaluate the duties of the Operations Support Specialist for proper segregation of duties.

SCOPE

The audit focused on the system of internal controls in place as of February 10, 2003. We tested data generated between July 1, 2002 and March 31, 2003. We did not review the help desk procedures, since that area was audited in 2001. In addition, we did not review the AS400 System Programmer's duties or the disaster recovery plan.

METHODOLOGY

We evaluated the physical security over the Operations Center by observing the operation of the area and identifying security measures, such as locks and keypad entry. We also interviewed and observed Operations staff in order to document our understanding of the risks involved and the procedures followed to mitigate those risks. Based on our understanding of the existing controls, we developed tests to confirm that the controls were being followed and were operating as intended.

RESULTS

We determined that the physical security in the Operations area is adequate; that access to and distribution of reports and other output containing sensitive information was adequately controlled; and that the tape management system was effective in controlling and tracking tape movements. Over the course of our audit, we noted the following areas where controls could be strengthened:

Finding 01 – Segregation of Duties

The Department of Technology uses IBM's software program Resource Access Control Facility (RACF) to manage access to the mainframe. We reviewed user access levels and noted the following:

- The RACF user ID, IBMUSER, has not been revoked and is currently being utilized by System Programmers. According to IBM's RACF Auditor's Guide, the user ID cannot be deleted, but the user ID should be revoked, so that another user cannot use it.

- There was incompatible access attributes assigned to two user IDs. The IDs had "Special", "Operations", and "Auditor" user attributes. According to the RACF Auditor's Guide, a Systems Administrator should not have the "Auditors" attribute because it allows the Systems Administrator to specify logging options, audit the security controls, and audit the use of system resources. These access rights are incompatible with the powerful access rights associated with the "Special" and "Operations" user attributes. Having all three attributes would allow a Systems

Administrator to range anywhere in the system, modify programming and data, and then delete any history of his or her activities in the audit logs.

- Two generic user IDs were established for the purpose of allowing Operations Support Specialists to respond to user requests to reset passwords. Having two user IDs allowed two Specialists to respond to help calls at the same time. The sharing of user IDs weakens system security, since activity associated with a given ID cannot be specifically attributed to one person. In this case, the two generic user IDs also had the “Special”, “Operations”, and “Auditor” user attributes. As we noted earlier, these are very powerful rights that are incompatible due to the ability it provides the holder to control all aspects of system security. These access rights also exceed what is necessary for the Operations Support Specialists to perform their jobs.

We did not note anywhere in our testing that employees abused their access privileges, nor did we find any appearance of impropriety. In fact, we believe some users were unaware of the extent of the access rights they held.

Agreed Upon Action 01– Segregation of Duties

The IBMUSER user ID will be revoked and programmers will not be allowed to sign on using the IBMUSER ID. The “Auditor” attribute will be removed from those user IDs that have incompatible rights. The Department of Technology will evaluate the logging options needed to monitor access levels and user activity. This information will be provided to the Security Administrator, so the appropriate RACF reports can be requested and reviewed for appropriate user activity and access levels. The two generic user IDs for resetting passwords will be deleted and the password reset function will be added to each Operations Support Specialist’s rights. At the end of each shift, an Operations Support Specialist will run a report that lists all password resets performed during the shift.

Finding 02 – Job Releases

As a means of ensuring the integrity of computer applications used by city departments in their day-to-day work, the Department of Technology uses a test region to modify program modules. Programmers move a copy of the application module and its related data into the test region, where they can test changes without the possibility of corrupting the original data or disrupting the work of user departments. Once modifications have been fully tested and are ready for release, a Systems Analyst reviews the work to ensure quality. Once approved by the Analyst, the Operators “release” the modified module into production, in essence replacing the original module. The CSSD030A report is printed daily and lists all module movements for the day. The Enterprise Operations Administrator is supposed to review the report and verify all releases were properly authorized and appear to be proper. During our test work we noted that the CSSD030A reports were not retained for six months as dictated by department policy (October, November, and most of December's reports were missing). We also noted that the CSSD030A reports did not list all of the modules released to production.

Agreed Upon Action 02 – Job Releases

The CSSD030A reports will be moved to the laser vault for storage. The laser vault is an online reporting system for the storage of electronic documents. This should ensure that the reports are not misplaced or accidentally discarded. In addition the utility program will be modified so that the report will list all module movements.

Finding 03 – Media Center

The Department of Technology has various media equipment that employees can borrow for work related purposes. The user must sign a user acceptance sheet before the media equipment will be issued to the user. Lotus Notes is utilized to maintain a current inventory of the media equipment.

We performed a physical inventory and noted that two overhead projectors were located in the media center and were not listed in the inventory. In addition we noted that the Operations Support Specialists do not check off any forms when the user returns the media equipment. This could allow users to falsely claim that they have returned equipment or make employees liable for equipment which was already returned. The current media center user agreement does not state that users are responsible for removing any files that they may have created on the media equipment. This could lead to an increased number of files cluttering the media center's laptop equipment, and could increase the risk that confidential or sensitive information would be viewed by unauthorized persons.

Agreed Upon Action 03 – Media Center

Once a year an Operations Support Specialist will conduct a physical inventory of the media center to ensure all equipment is accounted for and listed in the Lotus Notes database. The media center agreement will be revised so there will be an additional signature line for the users to sign when they return the equipment. There will be a section added that states it is the user's responsibility to remove any files that they have created on the equipment. In addition when the equipment is returned, the Operations Support Specialists will ensure that all parts are returned.

CONCLUSION

Based on the results of our audit work, we believe the physical security, tape management system, job scheduling, and output distribution was well controlled. The controls over the segregation of duties, job releases, and the media center could be strengthened.

We would like to thank the Operations Center for their cooperation and assistance during the audit.

Drew Harmon, CPA, CIA
Municipal Auditor

Michael J. Tuck, CPA, CGAP
Assistant Municipal Auditor

Pamela C. Mosdell, CISA, CIA
Information Systems Auditor